


<p>CAMPUS POLICY</p>  <p>UNIVERSITY OF COLORADO at COLORADO SPRINGS</p>	<p>POLICY NUMBER: 700-003</p>	<p>PAGE NUMBER: 1 of 13</p>
	<p>CHAPTER: Information Technology</p>	
	<p>SUBJECT: Information Technology Security</p>	
	<p>EFFECTIVE DATE: February 1, 2006</p>	
	<p>SUPERSESION:</p>	
<p>OPR: Chancellor</p> <p>VC:</p>	<p>Approved by Pamela Shockley-Zalabak, Chancellor, on February 1, 2006</p>	

I. POLICY

This policy is to help ensure the security and availability of information technology systems and networks and the confidentiality and integrity of electronic information captured, maintained, and used by UCCS. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by UCCS related to information systems and data security.

II. AUTHORITY FOR CAMPUS POLICIES

Authority for the creation of campus administrative policies is found in *The Laws of the Regents*, 1990, Article 3 Section B.8, which states:

The chancellor of the University of Colorado at Colorado Springs shall be the chief academic and administrative officer responsible to the president for the conduct of affairs of the Colorado Springs campus in accordance with the policies of the Board of Regents. The chancellor shall have such other responsibilities as may be required by these *Laws*, the Board, and as may be delegated by the president.

III. PURPOSE

The University of Colorado at Colorado Springs (UCCS) is a public institution with custodial responsibilities for a significant and diverse amount of sensitive information. UCCS is also a major research center that harbors a vast amount of valuable intellectual property, is the recipient of many federal and private grants, and holds business contracts with a broad range of public and private organizations. All of these roles place significant responsibilities on UCCS regarding the management and use of its information systems resources.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 2 of 13
--	--	--------------------	--------------------------------	--------------------------

The purpose of this policy is to help ensure the security and availability of information technology systems and networks and the confidentiality and integrity of electronic information captured, maintained, and used by UCCS. This policy provides direction for compliance with federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for confidential records associated with UCCS operations. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by UCCS related to information systems and data security.

IV. DEFINITIONS

The following terms are found in this policy document or its associated guideline documents:

Access Control: A physical, procedural, and/or electronic mechanism that ensures only those who are authorized to view, update, and/or delete data can access that data.

Authentication: A systematic method for establishing proof of identity.

Authorization: The process of giving someone permission to do or have something. System administrators/owners and data custodians define for their systems which users are allowed access to those systems and what privileges are assigned. A system could be an operating system, database, or application.

Availability: The assurance that a computer system is accessible by authorized users whenever needed or as pre-defined.

Common Criteria for Information Technology Security Evaluation: A comprehensive specification (aligned with the ISO IS 15408) that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.

Confidentiality: An attribute of information. Confidential information is sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial.

Cookie: A small text file that is sent to a user's computer by the server that the user is visiting. This file can record preferences and other data about the user's visit to a particular site. Cookies often are used for long-term data collection. Short-term cookies might be used for things like authentication in "single sign-on" services.

Cost-effective: To deliver desired results in beneficial financial terms.

Critical Servers: Within UCCS, critical servers are devices needed to support major UCCS administrative services, or they are devices that contain personally identifiable information that has value in and of itself.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 3 of 13
--	--	--------------------	--------------------------------	--------------------------

Data Custodians: Individuals who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of UCCS.

Decryption: The process of turning unreadable cipher text into readable text.

Encryption: The process of turning readable text into unreadable cipher text.

Firewalls: Policy-based filtering systems (composed of both hardware and software) that control and restrict the flow of data between networked computer systems. Firewalls establish a physical or logical perimeter where selected types of network traffic may be blocked. Blocking policies typically are based on computer IP addresses or protocol type of application (e.g., Web access or file transfer). Types of firewalls relevant to this policy include:

- Integrated OS (operating system) firewalls, bundled with the OS (e.g., Windows, Linux)
- Dedicated firewalls protecting labs or server sanctuaries
- Dedicated firewalls protecting individual hosts
- Logical firewalls protecting non-co-located systems

Forensics (Computer): The discipline of dissecting computer storage media, log analysis, and general systems to find evidence of computer crime or other violations.

Incident Response Capability: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source.

Information Systems: UCCS electronic information systems and data assets. All computing systems, networks, digital information, and other electronic processing or communications related resources or services provided through UCCS.

Integrity: Data or a system remains intact, unaltered, and reliable.

Intrusion Detection: A security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Non-repudiation: A mutually agreed upon process, secured evidence, or other method of operation that provides proof of receipt or protection from denial of an electronic transaction or other activity.

Off Site: A location separate and distinct from the area in which something, such as a computer, is located-- Frequently referred to when considering backup storage.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 4 of 13
--	--	--------------------	--------------------------------	--------------------------

Ownership: The term that signifies decision-making authority and accountability for a given span of control.

Perimeter Security: The ability to protect the outer limits of a network, or a physical area, or both.

Personally Identifiable Information: Specific data, elements of non-specific aggregate data, or other information that is tied to, or otherwise identifies, an individual or that provides information about an individual in a way that is reasonably likely to enable identification of a person as an individual and make personal information about them known.

Principle of Least Privilege: Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Principle of Separation of Duties: Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

Privacy: An individual's right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

Privacy Statement: Sometimes referred to as a privacy policy, a privacy statement is posted on an organization's Web site to notify visitors of the types of information being collected and what will be done with the information.

Risk Management: A comprehensive methodology that strives to balance risks against benefits in a pre-defined environment.

Security: An attribute of information systems that includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

Security Incident: An event during which some aspect of computer security is threatened.

Server Sanctuaries: Within UCCS, these are locations within computing facilities where clusters of sensitive or critical servers can be co-located and around which suitable physical and logical security measures can be implemented.

System: A network, computer, software package, or other entity for which there can be security concerns.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 5 of 13
--	--	--------------------	--------------------------------	--------------------------

System Administrators: Individuals who support the operations and integrity of computing systems and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. In addition, managing the computer network is often their responsibility in an inter-networked computing environment.

System Management: The activities performed by systems administrators.

System Operators: Individuals within the UCCS community who are accountable for the operational decisions about the use and management of a computing system. (See also *System Owners*.)

System Owners: Individuals within the UCCS community who are accountable for the budget, management, and use of one or more electronic information systems, electronic databases, or electronic applications associated with UCCS. (See also *System Operators*.)

Technicians: Individuals who have technical knowledge about computers, software, hardware, operating systems, and networks (e.g., system administrators, system engineers, or network engineers).

Users: Any individual who has been granted privileges and access to UCCS computing and network services, applications, resources, and information.

UCCS-owned Network: A network where network components (including active elements such as routers and switches, transmission media, and network-attached computers) are owned and operated by UCCS or units of UCCS. A message that travels over UCCS-owned networks is, in general, on an open network and hence requires additional security measures to be considered secure.

V. PROCEDURES

The following section sets forth the UCCS general policy regarding the security, availability, privacy, and integrity of its information systems, networks, and data. It stipulates specific policies for monitoring computing resources, managing electronic data and records, and controlling access to computing resources. In addition, it outlines minimum standards and practices for systems and network security.

a. General Statement of Policy

It is the policy of UCCS to ensure the security, availability, privacy, and integrity of its information systems, networks, and data and to ensure full compliance with all applicable federal and state statutes and regulations.

All providers and users of UCCS computing services, resources, and data are required to comply with all established policies, guidelines, and procedures, including applicable federal and state statutes and regulations.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 6 of 13
--	--	--------------------	--------------------------------	--------------------------

The general policy outlined in this section is the foundation for all other policy statements, guidelines, and procedures that are developed and implemented within UCCS computing environments.

b. Monitoring User Accounts, Files, and Access

UCCS does not routinely inspect or monitor the use of computers. However, the normal operation and maintenance of UCCS computing and network resources require authorized UCCS staff to back up and cache data and communications, log activity, monitor general usage patterns, and perform other activities that are necessary for the delivery and availability of service.

Receipt of a report or discovery of inappropriate or unauthorized use of computing and network resources may trigger monitoring and investigation by authorized UCCS staff.

UCCS systems owners and operators may specifically monitor the activity of individual users including files, session logs, content of communications, and Internet access without notice, when:

- The user's activity prevents access to computing and network resources by others.
- General usage patterns indicate that unacceptable activity is occurring.
- There is reasonable cause to believe that a user has violated or is violating policy or law.
- It appears necessary to do so to protect the UCCS from liability.
- It is required by and consistent with law.

Evidence of misuse of computing resources will be referred to appropriate UCCS officials. Evidence of possible criminal activity, which could include user files, email, and/or activity logs, will be turned over to appropriate UCCS and law enforcement officials.

c. Electronic Data and Records Management

Much of the vast amount of electronic data generated throughout the University comprises official UCCS records and requires specific management and handling practices and procedures as defined by UCCS and state law.

All UCCS system owners, operators, data custodians, and users are obligated to understand the nature of the data they generate, use, or store and to ensure that they are managing that data in full compliance with all state laws and UCCS records management policies. All UCCS system owners, operators, data custodians, and users are required to properly manage and protect electronic data they may be using, transmitting, and storing. Specific information regarding what is defined as an official record of UCCS, as well as retention, destruction, and archival requirements, is available through University of Colorado at Colorado Springs.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 7 of 13
--	--	--------------------	--------------------------------	--------------------------

The University privacy officer and the *CU Electronic Information Privacy Policy on Personally Identifiable Information* are the primary sources for direction and information regarding personally identifiable information.

The document named *UCCS Guidelines for Implementing Systems and Data Security Practices* contains a table of security measures commensurate with data categories.

d. Access Controls

UCCS has many different computing environments hosted on University networks, and within UCCS departments, schools, and business units. These environments require different security measures. Consequently, access control measures required for establishing users' access to any UCCS computing resources should be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All system owners, operators, and data custodians are responsible for ensuring that their systems are properly protected with appropriate access control measures based on the criticality of their systems and the data involved. The document named *CU Guidelines for Implementing Systems and Data Security Practices* provides direction on how to define the appropriate security measures for computing systems.

In addition, all computing systems hosted on UCCS networks must support and comply with the following fundamental access control measures, functions, and operating principles:

- Systems are required to have an access control mechanism that allows for an appropriate level of authorization and allocation of system and data resources to individual users. Access mechanisms can be physical, transaction-based, role-based, time-based, user-based, or use any other reasonable control method appropriate for the systems' functions.
- Shared systems are required to have the capability to log basic information about user access activity and to create historical logs and access violation reports.
- System access accounts for users must be based on a unique identifier, and no shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained.
- Users' system access must be based on the principle of least privilege and the principle of separation of duties.
- Computer applications must be developed and integrated in a way that maintains individual user accountability and audit capability.
- Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 8 of 13
--	--	--------------------	--------------------------------	--------------------------

e. Systems and Network Security

In light of the complex and diverse nature of the different computing environments hosted on UCCS networks and the wide range of statutory and regulatory compliance requirements, all systems and network security measures must be based upon the functional nature and degree of criticality of the computer systems, network resources, and data involved. All system owners and operators are responsible for ensuring that they have implemented all necessary security measures. Failure to do so risks creating security breaches or other incidents and could lead to temporary restrictions or even suspension of access to UCCS network resources.

The document named *CU Guidelines for Implementing Systems and Data Security Practices* provides direction on how to define the appropriate security measures for computing systems.

f. Systems Security—Minimum Measures and Practices

To protect the availability and integrity of UCCS computing resources, all computing systems and servers hosted on UCCS networks should comply with the following systems security measures and practices:

- Operating systems and applications must be maintained with the timely application of all related vendor-issued patches necessary to prevent the systems from being compromised and/or causing disruptions of network services and/or other systems.
- Externally accessible systems must install antivirus software and maintain procedures for regular signature updates.
- Shared systems are required to have a technical access control mechanism that allows authorization and allocation of system and data resources to individual users.
- Procedures must be maintained for regular backup of all data and system files necessary for discovery and recovery purposes. All backup media should be stored properly in a location authorized by the data owner with protections that allow access to the data by authorized personnel only. The ability to recover data from backups should be tested regularly.
- Shared systems are required to have the capability to log basic information about user access activity, system changes, and events for the possible creation of historical logs and access violation reports. Logs must be monitored for intrusions or attempts at unauthorized access.
- Systems must maintain a functioning and accurate system clock, since it is a critical element for the computer forensics and system logs that are essential for successful investigations.
- Encryption capabilities (the ability to turn readable text into unreadable cipher text) must be used for systems that send or receive personally identifiable information that is transmitted over open networks like the Internet or UCCS networks.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 9 of 13
--	--	--------------------	--------------------------------	--------------------------

Critical servers must be housed in protected areas such as server rooms (locations where suitable physical and logical security measures can be implemented).

Network Security—Minimum Measures and Practices

To protect the security, availability, and integrity of UCCS network resources, all computing systems and servers hosted on UCCS networks should comply with the following security measures and practices:

- Support proactive vulnerability probing and reporting by UCCS authorized technicians to help manage system security needs.
- Use secure protocols (e.g., SSL/SSH/Kerberos) for accessing all services that require authentication.
- Report all security breaches to the UCCS Information Technology Department.

Display security-warning banners prior to allowing the access log-on process to be initiated on systems running applications that are accessible on the UCCS-owned network. These security banners must inform all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.

g. Physical Security

Physical security measures are an important part of any effort to protect information system assets and services. As with logical security measures at UCCS, the physical security measures required for protecting UCCS computing resources must be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved.

UCCS has a wide spectrum of information systems deployments. They include:

- Large data-center facilities.
- Modest-sized server rooms.
- Small sets or individual departmental servers located in all manner of office environments.
- Computer labs.
- Telecommunications closets and vaults of all shapes and sizes.
- Media storage areas.
- Desktop computer workstations and printers.
- Wireless and mobile systems.

These technology deployments require different physical security measures. These measures are especially important when sensitive information is involved. All system owners and operators are responsible for ensuring that they have implemented the appropriate physical security measures for their particular computing environment. All users are required to respect the physical security measures in place.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 10 of 13
--	--	--------------------	--------------------------------	---------------------------

The following physical security measures and objectives should be implemented where applicable to protect UCCS computing and network assets and sensitive information:

- Physical access control measures sufficient to prevent UCCS assets from unnecessary and unauthorized access, use, misuse, vandalism, or theft.
- Computer rooms and telecommunications closets located away from heavy traffic patterns and not advertised.
- When appropriate, physical security measures should be in accordance with standards specified in the current edition of the National Fire Protection Association (NFPA) publication No. 75, *Protection of Electronic Computing/Data Processing Equipment*, and by Occupational Safety & Health Administration (OSHA) Safety and Health Standards. This is particularly important for data-center facilities.
- Certified smoke and fire-alarm and fire-suppression systems for data centers, server rooms, telecommunication closets, and vaults to mitigate potential damage to UCCS assets in the event of a fire.
- Environmental control measures (e.g., power supply, heating, ventilation, air conditioning, plumbing, and physical location) sufficient to protect UCCS assets from preventable service disruptions or harm.
- Departmental and general access labs monitored and secured when not open for use.
- Inventory control measures (e.g., asset tags or other identification markings) for tracking and accounting for UCCS assets.
- Secured off-site data/media storage and procedures that meet all archival, backup, and recovery needs for UCCS computing and network operations.
- Specific procedures for users of UCCS laptops, wireless services, and other mobile computing devices such as PDA's to prevent the theft or compromise of these devices.

Tools, systems, or procedures implemented to meet physical security requirements should be selected based on their cost-effectiveness and appropriate level of ability to protect UCCS assets.

h. Measures for Vendors

Vendors with access to computers and networks should meet many of the same standards placed on employees. They should understand the security policies and practices. Their access should be limited to just what is necessary for them to meet their contract requirements. When appropriate, vendors should be escorted into physically restricted areas. When their job is complete, they should return all access devices, and their log-on privileges should be terminated.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 11 of 13
--	--	--------------------	--------------------------------	---------------------------

i. Personnel Security Measures

This section outlines security measures and procedures that should be established and maintained when working with UCCS personnel throughout the employment process and when dealing with vendors, contractors, and temporary employees.

j. Measures for Hiring Employees

Comprehensive pre-employment screening is recommended for all potential candidates for key technical positions when those positions include an actual or potential wide span of systems control, and/or access to sensitive information, especially personally identifiable information or UCCS financial information. This screening could include checking and confirming references, background checks for criminal convictions (both federal and local, as necessary), and reviewing educational records and credit reports. All hiring officials should consider using such screening practices when hiring for key technical positions, regardless of employee type (contract, classified, professional, academic, or temporary).

All pre-employment inquiries must be conducted in full compliance with official UCCS guidelines established by UCCS Human Resources and in full compliance with state and federal laws. All hiring officials, managers, or others must work closely with UCCS Human Resources when engaging in any hiring process.

All UCCS departments, colleges, schools, and business units should have procedures in place to provide new employees with information about user responsibilities and guidelines associated with their assigned computer and network privileges and resources, including access to this document and related departmental policies, procedures, and guidelines. Appropriate supervision of new employee access to systems and data should be standard practice. New employees should be made aware that secure computing practices will be part of their performance reviews.

All physical and logical access to computing and network facilities and resources should be assigned in accordance with the principle of least privilege and principle of separation of duties.

k. Measures for Separating Employees

All UCCS departments, colleges, schools, and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is separated, even if the employee is going to another job within UCCS. These processes and procedures should include the following:

- The separated employee's immediate manager is responsible for notifying all system owners and operators, or the designated system administrator handling the

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 12 of 13
--	--	--------------------	--------------------------------	---------------------------

computer or communications accounts, to close all related accounts and remove all access capabilities related to the separated employee.

- Separated employees may not retain, give away, or remove from UCCS premises any UCCS information (electronic or hard copy) other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other UCCS information in the custody of the departing employee must be turned over to the employee's immediate supervisor at the time of departure.
- At the time of separation, all UCCS property must be returned. This includes portable computers, printers, modems, software, cellular telephones, digital pagers, PDA's, documentation, building keys, lock combinations, encryption keys, and access cards.

I. Measures for Employees on Leave or Suspension

All UCCS departments, colleges, schools, and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is suspended or is taking an extended leave of absence (including long-term illness or disability). It is important to use the same security measures for suspended employees as are used for separating employees. In addition, extended leaves of absence may require these measures, at the supervisor's discretion, taking into consideration such factors as level of access, nature and scope of computer applications and permissions, and duration of absence.

m. Policy Enforcement

Individuals who violate this policy may be denied access to UCCS computing and network resources and may be subject to other penalties and disciplinary action within and outside UCCS. Departmental managers are expected to work with appropriate UCCS resources in investigating and addressing suspected violation of this policy. Such resources include, but are not limited to, CU Internal Audit, CU Risk Management, UCCS Police Department, departmental managers, UCCS Human Resources, and Student Affairs.

UCCS may temporarily suspend, block, or restrict access to computing resources and accounts at any time when it reasonably appears necessary to do so in order to protect the integrity, security, or availability of UCCS computing and network resources or to protect UCCS from liability. UCCS will refer suspected violations of applicable law to appropriate law enforcement agencies.

In general:

- If violations of this policy are minor and unintentional, UCCS will take appropriate actions to resolve the issue, and violators may be subject to disciplinary measures.

CHAPTER: 700 Information Technology	SUBJECT: Information Technology Security	POLICY: 700-003	EFFECTIVE: February 1, 2006	PAGE: Page 13 of 13
--	--	--------------------	--------------------------------	---------------------------

- If violations of this policy are a result of negligent or deliberate acts, UCCS will take appropriate actions to resolve the issue including disciplinary measures up to and including termination of employment or expulsion.
- In addition to any other measures taken, if violations of this policy are a result of suspected illegal activities, UCCS will notify appropriate University authorities and law enforcement agencies.

UCCS reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of violations of this policy.

n. Policy Maintenance

This policy and the related guidelines will be reviewed yearly. A major security compliance audit must take place every three years.

VI. RESPONSIBILITY

- A. The chancellor or designee is responsible for ensuring that all campus policies are current, compliant with all statutory requirements, case law, and consistent with other applicable standards, including the *Laws of the Regents*, and the University of Colorado Administrative Policy Statements.
- B. The director of IT, the IT Advisory Council and the IT Leadership Team shall be responsible to:
 1. Review and update the security policy annually.
 2. Ensure their staff and colleagues are made aware of all applicable University and campus policies.

VII. ATTACHMENTS: